Local Distinguishability and Schmidt Number of Orthogonal States

Ping-Xing Chen,[1,2] Wei Jiang,[1] Zheng-Wei Zhou,[1] and Guang-Can Guo[1]

[1] *Key Laboratory of Quantum Communication and Quantum Computation, University of Science and Technology of China, Hefei 230026, People's Republic of China*

[2] *Department of Physics, National University of Defense Technology, Changsha, 410073, People's Republic of China*

(Dated: February 9, 2008)

Now, the known ensembles of orthogonal states which are distinguishable by local operators and classical communication (LOCC) satisfy the condition that the sum of Schmidit numbers of the orthogonal states is not bigger than the dimensions of the whole space. A natural question is whether an arbitary ensembles of LOCC-distinguishable orthogonal states satisfies the condition. We first show that, in this paper, the answer is positive. Then we generalize it into multipartite systems, and show that *a necessary condition for LOCC-distinguishability of multipartite orthogonal quantum states is that the sum of the least numbers of the product states (For bipartite system, the least number of product states is Schmidit number) of the orthogonal states is not bigger than the dimensions of the Hilbert space of the multipartite system.* This necessary condition is very simple and general, and one can get many cases of indistinguishability by it. It means that the least number of the product states acts an important role in distinguishablity of states, and implies that the least number of the product states may be an good manifestion of quantum nonlocality in some sense. In fact, entanglement emphases the "amount" of nonlocality, but the least number of the product states emphases the types of nonlocality. For example, the known W states and GHZ states have different least number of the product states, and are different in type.

PACS numbers: 03.65.Ud, 03.67.-a

Taking bipartite systems as examples, distinguishing locally orthogonal quantum states can be discribed as: Alice and Bob hold a part of a quantum system, which occupies one of m possible orthogonal states $\{|\Psi_i\rangle, i = 1, ..., m\}$. Alice and Bob know the precise form of these states, but don't know which of these possible states they actually hold. To distinguish these possible states they will perform some local operations and classical communication (LOCC): Alice (or Bob) first measures her part. Then she tells the Bob her measurement result, according to which Bob measures his part, and so on. With these measurement results they can exclude some or all possibilities of the system [1]. Obviously, the possible states can be distinguished if the global measurements are allowed. But they may not be distinguishable if only LOCCs are allowed. The fact that some orthogonal quantum states cannot be distinguished by LOCC is one of the interesting manifesties of non-locality in quantum mechanics. On the other hand, from the point of view of informaton, distinguishing locally orthogonal quantum states can also be imagined as: a information resource Charles owns two particles and encodes information using m possible orthogonal states of two particles, then Charles sends one of the particles to Alice and the other to Bob. Alice and Bob do rounds of LOCC to gain the encoded information. So distinguishing locally orthogonal quantum states is to gain information by LOCC, in essence.

There are much attentions on distinguishing locally quantum states [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11] and gainning locally information [12, 13]. Bennett et al showed that there are nine orthogonal product states in a $3 \otimes 3$ system which cannot be distinguished by LOCC [2]. Walgate et al showed that any two multipartite orthogonal states can be distinguished by LOCC [1]. For two-qubit systems (or $2 \otimes 2$ systems), any three of the four Bell states cannot be distinguished by LOCC if only a single copy is provided [4]. References [12, 13] discuss the rules of gaining locally information. LOCC-distinguishability of orthogonal states is related to many important directions in quantum information, such as distillable entanglement [10, 11, 14], quantum cloning, hiding information [15], quantum channel (See Ref. [6] and references therein), and quantum information basic theory (See Refs. [16] and references therein).

In spite many results, the complex nature of LOCC-distinguishability is far from clear. Now, the known ensembles of orthogonal states which are LOCC-distinguishable have a common feature that the sum of Schmidit numbers of the orthogonal states is not bigger than the dimensions of the whole space. For example, the ensembles of Bell states in Ref. [8] and the ensembles of orthogonal states in an $2 \otimes n$ system [7] have this feature. A natural question is: whether an arbitary ensemble of LOCC-distinguishable states has this feature? In this paper, we will show the answer is positive. We first show that if orthogonal states of arbitrary ensemble are LOCC-distinguishable, each orthogonal state is a linear superposition of a set of linearly independent product states, and the number of the linearly independent product states is not less than the sum of Schmidit numbers (or the least number of the product states for multipartite) of the orthogonal states. Then we present a very simple but powerful ceriterion to judge indistin-

guishability of states: if the sum of Schmidit number (or the least number of the product states) of the orthogonal states is bigger than the dimensions of the space, the states are LOCC-indistinguishable. With this criterion one can get many cases of indistinguishability [4]. Finally we discussion the effect of average entanglement and output entanglement on the indistinguishability of states. The conclusions may be useful in discussing the distinguishability of orthogonal quantum states further, understanding the essence of nonlocality and discussing the distillation of entanglement and hiding information.

Any protocol to distinguish the m possible orthogonal states can be conceived as many successive rounds of POVMs and communication by Alice and Bob. The effect of these measurements and communication can be described by a set of operators $\{A_i \otimes B_i, i = 1, \cdots, M\}$ acting on the Alice and Bob's Hilbert space [17]. Each operator A_i(or B_i) is a product of positive operators and unitary maps corresponding to Alice's (or Bob's) measurements and ratations. If an outcome i occures, the measured state $|\Psi_j\rangle$ becomes

$$|\Psi_j\rangle \to A_i \otimes B_i |\Psi_j\rangle , \tag{1}$$

where $A_i \otimes B_i$ satisfies the complete relation

$$\sum_i A_i^+ \otimes B_i^+ A_i \otimes B_i = I. \tag{2}$$

According to the polar and singular value decompositions of operators [17, 18], operators A_i, B_i can be expressed as the product of a positive operator and an unitary operator, namely

$$A_i = u_{iA} A_i'; \qquad B_i = u_{iB} B_i' \tag{3}$$

$$\begin{aligned} A_i' &= c_1^i \left|\varphi_1^i\right\rangle_A \left\langle\varphi_1^i\right| + \cdots + c_{N_a'}^i \left|\varphi_{N_a'}^i\right\rangle_A \left\langle\varphi_{N_a'}^i\right| \\ 0 &< c_j^i \leq 1, j = 1, \cdots, N_a'; N_a' \leq N_a \end{aligned} \tag{4}$$

$$\begin{aligned} B_i' &= d_1^i \left|\eta_1^i\right\rangle_B \left\langle\eta_1^i\right| + \cdots + d_{N_b'}^i \left|\eta_{N_b'}^i\right\rangle_B \left\langle\eta_{N_b'}^i\right| \\ 0 &< d_j^i \leq 1, j = 1, \cdots, N_b'; N_b' \leq N_b \end{aligned} \tag{5}$$

where u_{iA} and u_{iB} are unitary; A_i' is diagonal positive operators and filtrations which change the relative weights of components $\left|\varphi_1^i\right\rangle, \cdots, \left|\varphi_{N_a}^i\right\rangle$, and similarly for B_i'. N_a and N_b is the dimensions of Alice's and Bob's Hilbert space H_a, H_b, respectively.

If operators $\{A_i \otimes B_i, i = 1, \cdots, M\}$ can distinguish perfectively the states $\{|\Psi_i\rangle, i = 1, ..., m\}$, then each operator $A_i \otimes B_i$ corresponding to outcome i "indicate" only a state, namely

$$A_{i(s)} \otimes B_{i(s)} |\Psi_i\rangle \neq 0; \tag{6}$$

$$A_{i(s)} \otimes B_{i(s)} |\Psi_j\rangle = 0, j \neq i \tag{7}$$

Eq (6) means $A_i \otimes B_i$ can indicate $|\Psi_i\rangle$, and Eq (7) means $A_i \otimes B_i$ indicates only $|\Psi_i\rangle$. Of course, it is possible that a possible states $|\Psi_i\rangle$ may be indicated by many operators. The lower index (s) of $A_i \otimes B_i$ denotes many operators indicating the state $|\Psi_i\rangle$.

Furthermore, operator $A_i \otimes B_i$ indicate only $|\Psi_i\rangle$ means that all states $|\Psi_j\rangle (j \neq i)$ are orthogonal to the subspace spanned by the bases $\left\{\left|\varphi_l^i\right\rangle_A \left|\eta_k^i\right\rangle_B, l = 1, \cdots, N_a'; k = 1, \cdots, N_b'\right\}$. So if operator $A_i \otimes B_i$ indicates only $|\Psi_i\rangle$, all the following $N_a' N_b'$ one-rank operators $\left\{c_l^i \left|\varphi_l^i\right\rangle_A \left\langle\varphi_l^i\right| \otimes d_k^i \left|\eta_k^i\right\rangle_B \left\langle\eta_k^i\right|, l = 1, \cdots, N_a'; k = 1, \cdots, N_b'\right\}$ indicate only $|\Psi_i\rangle$ (It is possibel that some of the one-rank operators indicate none of the possible states). Similarly, the other operators $A_j \otimes B_j$ $(j \neq i)$ also correspond to similar one-rank operators. Let $\{a_i \otimes b_i = e_i |\varphi_i\rangle_A \langle\varphi_i| \otimes |\eta_i\rangle_B \langle\eta_i|\}$ $(e_i > 0, i = 1, \cdots, M', M' \geq N_a N_b$) denote all these one-rank operators. Obviously these one-rank operators satisfy the complete relation $\sum_i a_i^+ \otimes b_i^+ a_i \otimes b_i = I_{N_a \otimes N_b}$. Moreover, one can carries out these one-rank operators by doing the consequent projective measurements unitary ratations after one has carried out the operators $\{A_i \otimes B_i, i = 1, \cdots, M\}$. For example, after one gets output i corresponding to operator $A_i \otimes B_i$, one can carries out one-rank operators $\left\{c_l^i \left|\varphi_l^i\right\rangle_A \left\langle\varphi_l^i\right| \otimes d_k^i \left|\eta_k^i\right\rangle_B \left\langle\eta_k^i\right|, l = 1, \cdots, N_a'; k = 1, \cdots, N_b'\right\}$ by doing two unitary ratations u_{iA} and u_{iB}, and doing local peojective measurements$\left\{\left|\varphi_l^i\right\rangle_A \left\langle\varphi_l^i\right|, l = 1, \cdots, N_a'\right\}$ and $\left\{\left|\eta_k^i\right\rangle_B \left\langle\eta_k^i\right|, k = 1, \cdots, N_b'\right\}$. Thus we can have the following Lemma, as shown in Ref. [6]

Lemma: If states $\{|\Psi_i\rangle, i = 1, ..., m\}$ can be distinguished perfectively by $\{A_i \otimes B_i, i = 1, \cdots, M\}$, they can also be distinguished by a set of one-rank operators $\{a_i \otimes b_i\}$.

Since $\sum_i a_i^+ \otimes b_i^+ a_i \otimes b_i = \sum_i e_i^2 |\varphi_i\rangle_A \langle\varphi_i| \otimes |\eta_i\rangle_B \langle\eta_i| = I_{N_a \otimes N_b}$, any state $|\Psi\rangle$ in the Hilbert space $H_a \otimes H_b$ is the linear superposition of the product states $\{|\varphi_i\rangle_A |\eta_i\rangle_B, i = 1, \cdots, M'\}$, namely, $|\Psi\rangle = \sum_i e_i^2 \langle\varphi_i|_A \langle\eta_i|_B \Psi\rangle \ |\varphi_i\rangle_A |\eta_i\rangle_B$. Owing to a operator $a_i \otimes b_i$ indicates no more than a possible state, let's name the product states $\{|\varphi_i\rangle_A |\eta_i\rangle_B, i = 1, \cdots, M'\}$ indicating product states (IPS). Each IPS are orthogonal to all possible states except for no more than one possible state.

Since non-orthogonal measurements are allowed, not all IPS are linearly indepentent to each other, in general. But we can always find $N_a N_b$ linearly indepedent IPS (LIIPS) $|LIIPS\rangle_j (j = 1, \cdots, N_a N_b)$ such that they form a set of complete nonorthogonal product bases of the space $H_a \otimes H_b$. All states in the space $H_a \otimes H_b$ is the linear superposition of the LIIPS. Obviously, the number of LIIPS in a state $|\Psi_i\rangle$ is at least the Schmidt number of the state. Furthermore, if states $\{|\Psi_i\rangle, i = 1, ..., m\}$ can be distinguished perfectively by LOCC, each LIIPS

exists in no more than one possible state. So if states $\{|\Psi_i\rangle, i = 1, ..., m\}$ can be distinguished perfectively by LOCC, the sum of the numbers of the LIIPS in all possible state is not less than the sum of the Schmidt numbers of the possible states. Thus we have proven following Theorem.

Theorem 1: If states $\{|\Psi_i\rangle, i = 1, ..., m\}$ can be distinguished perfectively by LOCC, the number of LIIPS in a possible state $|\Psi_i\rangle$ is not less than the Schmidt number of the $|\Psi_i\rangle$, and then the number of LIIPS in all possible state is not less than the sum of the Schmidt numbers of the possible states.

Frome Theorem 1 we can get a interesting conclusion:

Theorem 2: If a set of orthogonal states $\{|\Psi_i\rangle, i = 1, ..., m\}$ in a Hilbert space shared by Alice and Bob can be distinguished perfectively by LOCC, the sum of Schmidt numbers of the states is not bigger than the dimensions of the space.

Proof: The proof is very simple. If the orthogonal states $\{|\Psi_i\rangle, i = 1, ..., m\}$ are LOCC distinguishable, and the sum of Schmidt numbers of the states is bigger than the dimensions of the space, then from Theorem 1 we can follow that the number of LIIPS is bigger than the dimensions N_aN_b of the whole space $H_a \otimes H_b$. This is impossible, and then completes the proof.

In the discussion above, the Schmidt number of a bipartite pure state is, in essence, the least number of product states of the pure state. So the results and their proof of Theorem 1 and 2 can be generalized into multi-partite system, obviously, if we replace "Schmidt number" by "the least number of product states" in a possible state. Thus we have that: *a necessary condition for distinguishability of multipartite orthogonal states is that the sum of the least numbers of product states of the orthogonal states is not bigger than the dimensions of Hilbert space of the multipartite system.*

From the theorem 2 one can get the many interesting cases. For example, for $n \otimes n$ systems one cannot distinguish deterministically $n + 1$ states, each of which has Schmidt number n [19]; for $n \otimes n$ systems, if one can distinguish n^2 orthogonal states, these states must be orthogonal product vectors as shown in Ref. [9]; for three qubits systems, three W-type orthogonal states are LOCC-indistinguishable (W-type states have the form of $a|001\rangle + b|010\rangle + c|100\rangle$).

As stated in the beginning, distinguishing locally orthogonal quantum states is related to gainning information by LOCC. Charles encodes information using orthogonal states $\{|\Psi_i\rangle, p_i, i = 1, ..., m, \}$ of two particles A and B, where p_i is the probability $|\Psi_i\rangle$ occures. Then Charles sends one of the particles to Alice and the other to Bob. Alice and Bob try to gain the encoded information by LOCC. The locally accessible information from the ensemble $\sigma = \{|\Psi_i\rangle, p_i, i = 1, ..., m, \}$ is limited by [12]

$$I_{acc}^{LOCC}(\sigma) \leq \ln(N_aN_b) - E, \tag{8}$$

and further by [13]

$$I_{acc}^{LOCC}(\sigma) \leq \ln(N_aN_b) - E - E_f, \tag{9}$$

where E is the average of the entanglement of σ; E_f is the average entanglement of the output.

Now we give a qualitative explanation of Eq (8) and (9). The state of the infinite copies of the ensemble, $\sigma^{\otimes n}(n \to \infty)$, is a mixture of $2^{nS(\sigma)}$ "likely" pure-states-strings with equal probability [20], where $S(\sigma)$ is von Neumann entropy. All Schmidt coefficient of the pure-states-strings are equal, and the Schmidt number of a string are 2^{nE}, where nE is the entanglement of each string. We now encode locally accessible information using these strings, namely, encode a locally accessible singnal using a string. From Theorem 1 and 2, one needs at least 2^{nE} LIIPS to encode a locally accessible singnal. So one can encode $\frac{(N_aN_b)^{\otimes n}}{2^{nE}}$ singnal at most in the spapce $(H_a \otimes H_b)^{\otimes n}$. Namely $I_{acc}^{LOCC}(\sigma^{\otimes n}) \leq \ln \frac{(N_aN_b)^{\otimes n}}{2^{nE}} = n(\ln(N_aN_b) - E)$. Obviously, $nI_{acc}^{LOCC}(\sigma) \leq I_{acc}^{LOCC}(\sigma^{\otimes n})$, thus we get Eq (8).

For one-rank operators, each output is a product state. If the output states are not product states, but entanglement states with average entanglement amount E_f, we can also explain Eq (9) by considering $\sigma^{\otimes n}(n \to \infty)$. After one has finished the operators to distinguish strings, one can get pure states the entanglement of each of which is nE_f. In this case the operators $\{A_i \otimes B_i, i = 1, \cdots, M\}$, which can distinguish the strings, are not the one-rank operators, but at least 2^{2nE_f}-rank ones. $A_i \otimes B_i$ project out an $2^{nE_f} \otimes 2^{nE_f}$ dimensions space, 2^{2nE_f} bases of which is LIIPS. Moreover, each string is indicated by at least 2^{nE-nE_f} operators of $\{A_i \otimes B_i, i = 1, \cdots, M\}$. So the LIIPS of each string is at least $2^{nE-nE_f}2^{2nE_f} = 2^{nE+nE_f}$, and then Alice and Bob can encode at most $\ln \frac{(N_aN_b)^{\otimes n}}{2^{nE+nE_f}} = n(\ln(N_aN_b) - E - E_f)$ bits locally accessible information in the space $(H_a \otimes H_b)^{\otimes n}$. Obviously, $nI_{acc}^{LOCC}(\sigma) \leq I_{acc}^{LOCC}(\sigma^{\otimes n})$, thus we get Eq (9).

LOCC-indistinguishability seem be related to entanglement. For example, Eq (8) and (9) imply that entanglement results in the indistinguishability. On the other hand, there are ensembles of LOCC-indistinguishable orthogonal *product* states [2, 3]. Moreover, one can destroy LOCC-distinguishability by reducing the average entanglement of the ensemble of states [9]. The two "opposite" results can be expained as shown in this paper: LOCC-indistinguishability is not related directly to average entanglement of orthogonal states, but to the least number of product states of the orthogonal states. LOCC-indistinguishability is related directly to average entanglement of orthogonal states at the limit of infinite number of copies of the ensemble.

In summary, we present a necessary condition for distinguishability of multipartite orthogonal quantum states, which is simple and general. With this condition one can get many cases of indistinguishability. These results mean that the least number of the product states acts an important role in distinguishablity of states. This implies that the least number of the product states may be an good manifestion of quantum nonlocality in some sense. In fact, entanglement emphases the "amount" of nonlocality, but the least number of the product states emphases the types of nonlocality. For example, the known W states and GHZ states have different least number of the product states, and are different in type.

The results in this paper open three interesting questions: 1. For ensembles of states which satisfy the condition in Theorem 2 but are still indistinguishable, whether the indistinguishability of the states results from the existence of the subspace the projections of the states on the subspace do not satisfy the condition? More precisely, is the following result ture? — if there is a subspace the sum of the Schmidt number of the projections of the states on the subspace is bigger than the dimensions of the subspace, the states are LOCC-indistinguishable. This supposed result is stronger than Theorem 2, obviously. If the supposition is ture, it approaches to a necessary and sufficient condition of LOCC-distinguishaility. 2. To our knowledge, no ensembles of bipartite states which can be distinguished by POVMs but not by projective measurement has been found, while the ensemble of multipartite states has been found [21]. Is it ture that if bipartite states can be distinguished by POVMs, they can be distinguished by projective measurements? 3. Eqs. (8) and (9) can be generalized into multipartite if we re-define E and E_f corresponding to the least number of product states in a pure state, in principle. But the detailed investigations into the generalization are necessary.

This work is supported by the National Natural Science foundation (No. Grants 10404039, 10204020), the Chinese National Fundamental Research Program (2001CB309300), the Innovation funds from Chinese of Academy of Sciences, and the China Postdoctoral Science Foundation.

[1] J.Walgate, A.J.Short, L.Hardy and V.Vedral,Phys.Rev.Lett.85,4972 (2000)

[2] C. H. Bennett, D.P. DiVincenzo, C.A. Fuchs, T.Mor, E.Rains,P.W. Shor, J.A. Smolin, and W.K. Wootters, Phys. Rev. A 59,1070 (1999) or quant-ph/9804053.

[3] C. H. Bennett, D.P. DiVincenzo, T.Mor, P.W. Shor, J.A. Smolin, and B. W. Terhal, Phys. Rev. Lett 82,5385 (1999).

[4] M. Horodecki, P. Horodecki, and R. Horodecki, Acta Physica Slovaca, 48, (1998) 141, or quant-ph/9805072

[5] S. Virmani, M.F. Sacchi, M.B. Plenio and D. Markham, Physics Letters A 288, 62-68 (2001);Y.-X.Chen and D.Yang, Phys.Rev.A 64, 064303 (2001)

[6] John Watrous, Phys. Rev. Lett 95, 080505 (2005)

[7] J. Walgate and L. Hardy, Phys. Rev. Lett 89, 147901 (2002)

[8] S.Ghosh, G.Kar, A.Roy, A.Sen and U.Sen, Phys.Rev.Lett.87, 277902 (2001); S. Ghosh, G.Kar, A.Roy, D.Sarkar, A.Sen(De) and U.Sen, Phys. Rev. A 65, 062307

[9] M. Horodecki, A. Sen (De), U. Sen and K. Horodecki, Phys.Rev.Lett.90, 047902 (2003)

[10] V. Vedral and M. B. Plenio, Phys. Rew A 57, 1619 (1998);

[11] V. Vedral M. B. Plenio, K. Jocobs and P. L. Knight, Phys. Rew A 56, 4452 (1997)

[12] P. Badziag, M. Horodecki, A. Sen(De) and U. Sen, Phys. Rev. Lett. 91, 117901 (2003).

[13] M. Horodecki, J. Oppenheim, A. Sen(De) and U. Sen, Phys. Rev.Lett. 93, 170503 (2004).

[14] S. Ghosh, P. Joag, G. Kar, S. Kunkri and A. Roy,arXiv:quant-ph/0403134 (2004); P.- X Chen and C.-Z Li, Quant. Inf and Comp,V3 203 (2003).

[15] P. Hayden, D. Leung, and G. Smith Phys. Rev. A 71, 062339 (2005).

[16] M. Horodecki, J. Oppenheim, A. Winter Nature 436, 673 (2005); M. Horodecki et al, Phys. Rev. A 71, 062307 (2005)

[17] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information (Cambridge University Press, Cambridge),pp. 78-79;

[18] M. Horodecki, P. Horodecki, and R. Horodecki,Phys. Rev. Lett. 80, 5239 (1998);N. Linden, S. Massar and S. Popescu, Phys. Rev. Lett. 81, 3279 (1998);W. K. Wootters, Phys. Rev. Lett. 80,2245 (1998)

[19] M. Nathanson, J. Math. Phys. (N.Y.) 46, 062103 (2005).

[20] C. H. Bennett, G. Brassard, S. Popescu and B. Schumacher, Phys. Rev. A 53, 2046 (1996).

[21] P.-X.Chen and C.-Z Li, Phys.Rev.A 70, 022306(2004).